數碼KEY 睇緊啲



HONG KONG MONETARY AUTHORITY
香 港 金 融 管 理 局








HKMAGOVHK


HKMAGOVHK

鳴謝: 香港銀行公會
Acknowledgement: The Hong Kong Association of Banks

什麼是個人數碼鎖匙？

在電子世界，帳戶及個人資料就是你的個人數碼鎖匙 (personal digital keys)，它跟你的家門鎖匙一樣重要，必須無時無刻都好好保管。這些資料一旦不小心落入不法之徒手中，對方有可能偽冒你登入你的網上/手機銀行或電子錢包（以下統稱「電子金融服務」）帳戶，令你遭受財務損失。緊記「**數碼Key 睇緊啲**」！

個人數碼鎖匙的例子



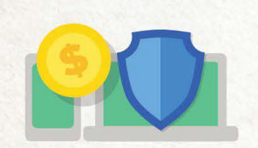
保護個人數碼鎖匙的實用貼士



如果在網上提供個人資料，例如在網購的時候，一定要了解清楚網站是否可靠。



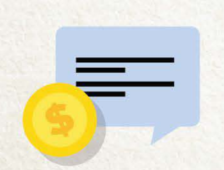
千萬不要透過不明Wi-Fi或公用電腦登入網上/手機銀行及電子錢包。



妥善地保護用以進行網上交易(包括電子金融服務)的電腦及手機。



在更換手機前，謹記刪除原有手機內的所有資訊。



注意銀行發出的手機提示訊息，若忽略訊息的話，可能帳戶被盜用了也不知道。



設定難以猜破的密碼，及要定期更改。不要所有電子金融服務的帳戶，都使用同一個密碼。



如懷疑個人資料被盜用，應立即通知銀行或電子金融服務營運商。

保護電腦及手機的要點



密碼

為你的電腦及手機設定難以猜破的密碼並定期更改，及在不同設備和網上服務設定不同的密碼。切勿與其他人分享你的密碼，並應啟動電腦及手機的自動上鎖功能。



安全系統及程式

使用最新版本的操作系統、網上/手機銀行、電子錢包流動應用程式（Apps）及瀏覽器，切勿用Jailbreak（越獄）或Root機等手法改裝手機及平板電腦。只從官方應用程式商店或可信的來源下載及升級Apps，並安裝最新的保安軟件和及時更新安全修補程式，及備份重要的資料。



提防惡意程式

點擊前請三思 - 切勿下載或開啟可疑的檔案、瀏覽可疑網站或開啟來歷不明（如電郵、即時通訊、短訊和二維碼）的超連結及附件。

時刻提高警覺，提防不法之徒偽裝成知名的商業網站或人物，或建立看似官方網站的欺詐網站或電郵，以誘騙用戶點擊相關的超連結或附件或其他形式，騙取用戶的個人資料。如有疑問，應透過直接輸入正確的網址瀏覽，避免點擊可疑的超連結。



網絡功能

關閉無需使用的無線網絡功能（如Wi-Fi、藍芽和NFC）。如需使用Wi-Fi，應只選用可靠及加密的網絡，並移除不必要的Wi-Fi連線設定。

使用電子金融服務的主要保安提示



登入過程

檢查登入網頁及過程有否異樣（如出現可疑的彈出視窗、被要求提供額外的個人資料）及是否有人窺看密碼，並在使用後馬上登出。



登入名稱及密碼

設定難以猜破及與其他網上服務不同的密碼，並定期更改。切勿將密碼記錄在電腦、手機或當眼位置，或隨便透露予第三方流動應用程式。

應盡可能選用雙重認證登入電子金融服務帳戶，並了解相關的操作。妥善保管用作進行雙重認證的設備（如保安編碼器或手機）。



付款及轉帳

在確認付款和轉帳之前，仔細檢查收款人資料（例如手機號碼、電郵、帳戶號碼及收款人姓名）是否正確。設置合適的交易限額。



電腦及手機

保護用以登入電子金融服務的電腦和手機。避免透過公用電腦或公共無線網絡登入。避免借用其他人的電腦/手機或讓其他人使用你的電腦/手機登入電子金融服務帳戶。



電子金融服務網址及應用程式

應直接輸入電子金融服務提供者的網址、書籤或相關的應用程式登入。切勿透過沒有預期或可疑的網站、電郵、網上的超連結或附件登入或提供個人資料（包括登入名稱及密碼、信用卡資料及一次性密碼等）。



銀行訊息

及時查閱銀行發出的手機短訊及其他信息，並查核交易紀錄。若發現可疑情況，應立即聯絡銀行。銀行職員一定不會以電話或電郵，要求提供任何敏感的個人資料（包括密碼）。



商業客戶的保安措施

公司應提醒員工如何識別釣魚郵件，及不要在社交媒體上分享個人的職務及機構的人事架構，以預防相關資料被用作詐騙。在公司系統設定合適的用戶權限。採用加密措施保護你的商業及客戶資料。

如收到電郵或電話要求更改匯款資料，或不尋常及緊急的付款要求，應提高警覺，並即時透過日常聯繫方式，主動向相關聯絡人或公司管理層查證有關請求。除非確定更改付款資料的要求是無誤，否則不要隨便作出更改。

12/2019